Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Pure and Applied Algebra 205 (2006) 189–209
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

Non-standard automorphisms and non-congruence subgroups of SL_2 over Dedekind domains contained in function fields

A.W. Mason[a,*], Andreas Schweizer[b]

[a] *Department of Mathematics, University of Glasgow, Glasgow, G12 8QW, Scotland, UK*
[b] *Korea Institute for Advanced Study (KIAS), 207-43 Cheongnyangni 2-dong, Dongdaemun-gu, Seoul 130-722, Korea*

Received 31 January 2005; received in revised form 16 June 2005
Available online 24 August 2005
Communicated by C.A. Weibel

Abstract

Let K be an algebraic function field of one variable with constant field k and let $\mathscr{C}$ be the Dedekind domain consisting of all those elements of K which are integral outside a fixed place ∞ of K. We introduce "non-standard" automorphisms of the group $SL_2(\mathscr{C})$, generalizing a result of Reiner for the special case $SL_2(k[t])$. For the (arithmetic) case where k is finite, we use these to transform congruence subgroups into non-congruence subgroups of almost any level. This enables us to investigate the existence, number, and minimal index of non-congruence subgroups of prescribed level. We provide also a group-theoretic characterization of those $SL_2(\mathscr{C})$ where $\mathscr{C}$ is a principal ideal domain.

MSC: 11F06; 19B37; 20F28; 20G30; 20H05

0. Introduction

Let K be an algebraic function field of one variable with constant field k. Let $\mathscr{C}$ be the ring of all elements of K that are integral outside a fixed place ∞ of K. (The simplest example is $\mathscr{C}=k[t]$, the polynomial ring over k.) Our focus of attention is the group $\Gamma=SL_2(\mathscr{C})$. When k is *finite*, $\mathscr{C}$ is the *only* example of an *arithmetic Dedekind domain* of non-zero characteristic

* Corresponding author.
E-mail addresses: awm@maths.gla.ac.uk (A.W. Mason), schweiz@kias.re.kr (A. Schweizer).

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2005.06.018

with finitely many units. (This is a well-known consequence of Dirichlet's Unit Theorem.) In this case the group Γ plays a fundamental role in the theory of Drinfeld modular curves [4], which extends to the function field setting the classical theory of modular forms.

Let V be a k-subspace of $\mathscr{C}$ and let $B_2(V)$ be the subgroup of all upper triangular matrices over V in Γ. Serre [14, Theorem 10, p. 119] has proved a fundamental decomposition theorem for Γ, valid for *any* k. From this it follows that Γ is the free product of $B_2(\mathscr{C})$ and another subgroup J, amalgamated along $B_2(V_0)$, where V_0 is a *finite dimensional* subspace of $\mathscr{C}$. (The dimension of V_0 is determined by the Riemann–Roch Theorem.)

Any k-automorphism of $\mathscr{C}$, ϕ, which fixes V_0, then gives rise to an automorphism, Φ, of Γ. This generalizes a well-known result of Reiner [13] for the special case $SL_2(k[t])$. Any *ring* automorphism of $\mathscr{C}$ extends (in a very natural way) to an automorphism of Γ and is often referred to as "standard". For this reason we refer to the above as "non-standard". Since, by definition, Φ maps elementary matrices onto themselves, it is appropriate to introduce the notion of the *quasi-level*, $ql(S)$, of a subgroup S of Γ. This extends the classical notion of the *level* of S, $l(S)$. By definition $ql(S)$ is an additive subgroup of $\mathscr{C}$ which in most cases is a k-subspace. Then $l(S)$ is the largest $\mathscr{C}$-ideal contained in $ql(S)$. The crucial point for our purposes is that the quasi-level of $\Phi(S)$ is equal to $\phi(ql(S))$.

For the remainder of the paper we assume that Γ is of arithmetic type, i.e. k is finite. Here the classical notion of the *level* of a subgroup has proved to be particularly useful, especially for the *congruence subgroups* of Γ. We use non-standard automorphisms to map congruence subgroups onto *non-congruence subgroups* of (almost) arbitrary quasi-level. By this means we prove, for example,

Theorem A. *Γ has uncountably many non-congruence subgroups of level zero.*

(This extends a result of Serre [14, p. 125] who has proved that Γ has uncountably many finite index subgroups.) The existence of such subgroups represents an anomaly in the following sense. If A is an arithmetic Dedekind domain, other than $\mathscr{C}$, it is known that every finite index subgroup of $SL_2(A)$ has non-zero level.

In previous papers the authors [10–12] have determined $ncs(\mathscr{C})$, the minimal index of a non-congruence subgroup of Γ. Now we use non-standard automorphisms to determine the minimal index of a non-congruence subgroup of prescribed level, in particular those of level zero and level $\mathscr{C}$, the extremal cases.

We derive a lower bound for the minimal index of a non-congruence subgroup of level different from $\mathscr{C}$. In "almost all" cases it turns out to be greater than $ncs(\mathscr{C})$. Under certain conditions our lower bound is sharp, for example

Theorem B. *Let $q \leqslant 3$. Then Γ has uncountably many normal subgroups of level zero and index q. Moreover, for every maximal ideal $\mathfrak{m}$ of sufficiently high degree there exists at least one normal non-congruence subgroup of Γ of level $\mathfrak{m}$ and index q.*

For $q > 3$ we can prove an analogous result (Proposition 4.5) only under the condition that $\mathscr{C}$ has an ideal of degree 1. The difference between the cases $q \leqslant 3$ and $q > 3$ (in the formulas and in terms of difficulty of proof) comes from the fact that for $q \leqslant 3$ all diagonal matrices are central, which allows an easy construction of subgroups of index q.

In contrast to the case of level zero we show that $ncs(\mathscr{C})$ can always be attained by a non-congruence subgroup of non-zero level, and in "almost all" cases even by a non-congruence subgroup of level $\mathscr{C}$. In the process we investigate also the number of such subgroups (i.e. whether finite, countably infinite or uncountably infinite). We also determine precisely which $\mathscr{C}$-ideals occur as levels of non-congruence subgroups.

Theorem C.

(a) *$SL_2(k[t])$ has no non-congruence subgroups of level $\mathfrak{a}$ if and only if* $\deg(\mathfrak{a}) \leqslant 1$. *If* $\deg(\mathfrak{a}) > 1$, *the number of non-congruence subgroups of level $\mathfrak{a}$ is countably infinite.*
(b) *Let $g = 0$ and $\delta = 2$. If $q \leqslant 3$, then there exist uncountably many normal non-congruence subgroups of level $\mathscr{C}$ and index q in Γ. But if $q > 3$, then Γ has no non-congruence subgroups of level $\mathscr{C}$. For any q there are infinitely many non-congruence subgroups of level $\mathfrak{a}$, for all $\mathscr{C}$-ideals $\mathfrak{a}$.*
(c) *If $g > 0$ or $\delta > 2$, then Γ has non-congruence subgroups of every non-zero level $\mathfrak{a}$.*

Serre's decomposition theorem [14, Theorem 10, p. 119] for Γ is derived from its action on a certain (combinatorial) *tree*, X (a special type of *Bruhat–Tits building*). Using the theory of groups acting on trees this theorem follows from the structure of the quotient graph $\Gamma\backslash X$. Serre [14, Theorem 9, p. 106] has proved that $\Gamma\backslash X$ consists of a "central" part adjoined to a number of *ends*. Moreover, these ends are in one–one correspondence with the elements of the *ideal class group* of $\mathscr{C}$, $Cl(\mathscr{C})$. By virtue of (LMQ) it is known precisely when $Cl(\mathscr{C})$ is trivial. In our final section we use a matrix version of Serre's theorem [9] to establish a *group-theoretic* property particular to those Γ for which $\mathscr{C}$ is a principal ideal domain.

Theorem D. *Γ has at most countably many finite index subgroups of non-zero level if and only if $\mathscr{C}$ is a principal ideal domain.*

The intuitive idea of the proof is the following. The group Γ is generated by finitely many elements corresponding to the central part of the graph $\Gamma\backslash X$ plus countably infinitely many ones for each end. Let $\Delta(\mathfrak{q})$ be the minimal subgroup of level $\mathfrak{q}$. In general, $\Delta(\mathfrak{q})$ has infinite index in Γ. Dividing Γ by $\Delta(\mathfrak{q})$ kills almost all of the generators corresponding to a certain end. Thus (for $\mathfrak{q}$ of sufficiently high degree) the group $\Gamma/\Delta(\mathfrak{q})$ is finitely generated if and only if there is no second end, i.e. if $\mathscr{C}$ has class number 1.

1. Notation

Throughout the paper we will use the following notation:

K an algebraic function field of one variable with constant field k,
g the genus of K,
∞ a chosen place of K,
δ the degree of the place ∞,
$\mathscr{C}$ the ring of all elements of K that are integral outside ∞,
Γ the group $SL_2(\mathscr{C})$.

Then $\mathscr{C}$ is a Dedekind ring whose group of units is k^*. It is known that $\dim_k(\mathscr{C}/\mathfrak{q})$ is *finite*, for all non-zero $\mathscr{C}$-ideals $\mathfrak{q}$. We denote this dimension by $\deg(\mathfrak{q})$. By definition k is *algebraically closed* in K. (See [15, Chapters I, III].) The simplest example is the polynomial ring $k[t]$. (Indeed this is the "basic" example in the sense that $k[t]$ is contained in every such $\mathscr{C}$.)

For the special case

$$k = \mathbb{F}_q,$$

where $\mathbb{F}_q$ is the finite field with q elements, it is known that $\mathscr{C}$ is the *only* example of an *arithmetic Dedekind domain* of non-zero characteristic with finitely many units. The results in Section 2 hold for all k. For nearly all of the remainder of the paper we assume that k is finite.

For each $\alpha \in k^*$, $c \in \mathscr{C}$, we put

$$L(\alpha, c) := \begin{bmatrix} \alpha & c \\ 0 & \alpha^{-1} \end{bmatrix}$$

and

$$T(c) := L(1, c) = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}.$$

For every subspace W of the k-vector space $\mathscr{C}$ we define

$$B_2(W) := \{L(\alpha, c) : \alpha \in k^*, c \in W\}$$

and its subgroup of unipotent matrices

$$U(W) := \{T(c) : c \in W\}.$$

It is easily verified that

$$\langle B_2(\mathscr{C}), SL_2(k)\rangle = E_2(\mathscr{C}),$$

where

$$E_2(\mathscr{C}) := \left\langle \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} : c \in \mathscr{C} \right\rangle$$

is the group generated by the elementary matrices.

For every ideal $\mathfrak{a}$ of $\mathscr{C}$ we define

$$\varDelta(\mathfrak{a}) := \text{the normal subgroup of } \varGamma \text{ generated by all matrices } T(c) \text{ with } c \in \mathfrak{a}.$$

Definition. The *level*, $l(S)$, of a subgroup S of $\varGamma$ is defined to be the largest ideal $\mathfrak{a}'$ in $\mathscr{C}$ such that $\varDelta(\mathfrak{a}') \subseteq S$. This includes the possibility $\mathfrak{a}' = \{0\}$ (which we refer to as *level zero*).

Of particular importance are the subgroups

$$\varGamma(\mathfrak{a}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \varGamma : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\mathrm{mod}\ \mathfrak{a}) \right\}.$$

It is clear that $l(\Delta(\mathfrak{a})) = l(\Gamma(\mathfrak{a})) = \mathfrak{a}$. It is well-known that

$$\Gamma/\Gamma(\mathfrak{a}) \cong SL_2(\mathscr{C}/\mathfrak{a}).$$

Restricting our attention for the moment to the case where $\mathscr{C}$ is an *arithmetic Dedekind domain*, a subgroup S of Γ is called a *congruence subgroup* if it contains a group $\Gamma(\mathfrak{q})$ for some non-zero ideal $\mathfrak{q}$ of $\mathscr{C}$. Since $\mathscr{C}/\mathfrak{q}$ is then finite, a congruence subgroup of Γ is necessarily of finite index. The other finite index subgroups of Γ are called *non-congruence subgroups*. Since $\mathscr{C}$ has countably many ideals, Γ has only countably many congruence subgroups. On the other hand, it is well-known [14, Lemma 11, p. 125] that Γ has uncountably many finite index subgroups. In particular, every finite index subgroup of level zero is clearly a non-congruence subgroup. (We will prove the existence of uncountably many such subgroups.)

We will make use of the following important property of the level of a congruence subgroup. The first version of this result (for the case of the classical modular group), due to Fricke, dates back to the 19th century.

Theorem 1.1 (*Grunewald and Schwermer [6, Theorem 2.5]*). *Suppose that k is finite. Let S be a subgroup of finite index in Γ. If $l(S) = \mathfrak{q}$ is non-zero, then S is a congruence subgroup if and only if $\Gamma(\mathfrak{q}) \subseteq S$.*

In [10–12] we determined

$$ncs(\mathscr{C}) := \text{the minimal index of a non-congruence subgroup in } \Gamma.$$

In all cases it turned out to be equal to $m(\Gamma)$, where

$$m(G) := \text{ the minimal index of a proper subgroup of a group } G.$$

In Sections 4 and 5 we will examine in much more detail the levels of subgroups attaining this minimal index.

2. Non-standard automorphisms

The results of this section hold for any k. Let v be the discrete valuation of K determined by ∞. For each non-negative integer n, we put

$$\mathscr{C}(n) := \{x \in \mathscr{C} : v(x) \geqslant -n\}.$$

Then $\mathscr{C}(n)$ is a *finite-dimensional* vector space over k, whose dimension is determined by the *Riemann–Roch Theorem*. (See [15, I.4.9, p. 18].) Obviously, $k \subseteq \mathscr{C}(n)$. In particular, $\mathscr{C}(0) = k$, by [15, I.1.19, p. 8].

We put

$$\Gamma_n := \{L(\alpha, c) : \alpha \in k^*, c \in \mathscr{C}(n)\} = B_2(\mathscr{C}(n)),$$

where $n \geqslant 0$. It is clear that, for all $n \geqslant 0$,

$$\Gamma_n \leqslant \Gamma_{n+1}.$$

We define

$$\Gamma_\infty := \bigcup_{n=0}^{\infty} \Gamma_n = \{L(\alpha, c) : \alpha \in k^*, c \in \mathscr{C}\} = B_2(\mathscr{C}).$$

Serre's decomposition theorem [14, Theorem 10, p. 119] shows that Γ_∞ is a (non-trivial) factor in a decomposition of Γ as an amalgamated product of a pair of its subgroups. We make use of a matrix version [9] of Serre's result. It is convenient to deal with the cases $g = 0$ and $g \neq 0$ separately.

Theorem 2.1. *Suppose that* $g \neq 0$. *Let* n_0 *be the smallest integer* n *such that*

$$\delta n \geqslant 2g - 1.$$

Then there exists a subgroup J *of* Γ, *such that*

$$\Gamma = \Gamma_\infty \mathop{*}_{H} J,$$

where $H = \Gamma_{n_0} = B_2(\mathscr{C}(n_0))$. *Moreover,*

$$\dim_k(\mathscr{C}(n_0)) = n_0\delta + 1 - g.$$

Proof. From the theory of groups acting on trees applied to the action of Γ on its Bruhat–Tits building it follows that

$$\Gamma = \Gamma_\infty \mathop{*}_{H} J,$$

where $H = \Gamma_{n_0}$, for some subgroup J. (See [9, Theorems 4.2, 5.1].) The dimension of $\mathscr{C}(n_0)$ follows from [9, Lemmas 1.2, 3.7]. □

We note that

$$g \leqslant \dim_k(\mathscr{C}(n_0)) \leqslant g + \delta - 1.$$

It follows, for example, that $\dim_k(\mathscr{C}(n_0)) = g$, when $\delta = 1$. In particular, when $g = \delta = 1$, then $\mathscr{C}(n_0) = k$ (as verified by Takahashi [16]).

Theorem 2.2. *Suppose that* $g = 0$. *Then there exists a subgroup* J *of* Γ *such that*

$$\Gamma = \Gamma_\infty \mathop{*}_{\Gamma_0} J.$$

Proof. We note that Lemma 3.7 in [9] holds for "$n = 1$", by [9, Lemma 1.2]. The result follows from [9, Theorems 4.2, 5.1], as in the proof of Theorem 2.1. □

Remark 2.3. Theorems 2.1 and 2.2 generalize the well-known result

$$SL_2(k[t]) = B_2(k[t]) \mathop{*}_{H} SL_2(k),$$

where $H = B_2(k)$, which is a version of Nagao's theorem. (See [14, Chapter II, Section 1.6] for a proof that uses the associated Bruhat–Tits tree.)

The fact that in this special case the group J is explicitly known (and finite if k is finite) is somewhat untypical. In most cases the group J will not be finitely generated. This comes from the fact that in the description of Γ in terms of stabilizers of vertices and edges of the quotient graph $\Gamma\backslash X$ of the Bruhat–Tits tree X, the Borel subgroup $B_2(\mathscr{C})$ corresponds to a cusp of $\Gamma\backslash X$ (i.e. an infinite half-line of vertices and edges), whereas J corresponds to the rest of the graph. In the special case $\mathscr{C} = k[t]$ this rest is merely one vertex.

Let $\phi : \mathscr{C} \to \mathscr{C}$ be any k-automorphism of the k-space $\mathscr{C}$, which fixes the elements of k. Then ϕ induces an automorphism Φ of Γ_∞ defined by

$$\Phi : L(\alpha, c) \longmapsto L(\alpha, \phi(c)),$$

where $\alpha \in k^*$, $c \in \mathscr{C}$.

The following is an immediate consequence of Theorems 2.1 and 2.2.

Theorem 2.4. *Let ϕ be any k-automorphism of $\mathscr{C}$ which fixes the elements of $\mathscr{C}(n_0)$. Define $\Phi : \Gamma \to \Gamma$ by*

$$\Phi(\gamma) = \begin{cases} L(\alpha, \phi(c)), & \gamma = L(\alpha, c), \\ \gamma, & \gamma \in J. \end{cases}$$

Then Φ is an automorphism of Γ.

This extends a well-known result of Reiner [13] for the special case $\mathscr{C} \cong k[t]$ (Cohn [1, Theorem 11.2] has proved an equivalent result for group $E_2(\mathscr{C})$). The automorphism Φ is "non-standard" in the following sense.

Any *ring*-automorphism ψ of $\mathscr{C}$ induces a "standard" automorphism Ψ of Γ, defined by

$$\Psi : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} \psi(a) & \psi(b) \\ \psi(c) & \psi(d) \end{bmatrix}.$$

Moreover, Γ has of course inner automorphisms. Other "standard automorphisms" as described in [13] do not occur, since there is no non-trivial homomorphism from Γ into k^*, and the contragredient (inverse of the transposed matrix) is obtained by conjugating with

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

As we shall see below it is easy to find automorphisms Φ as in Theorem 2.4 which are not contained in the group generated by the inner and the standard ring automorphisms.

3. Quasi-level

With some specified exceptions the results of this section hold for all k. We apply non-standard automorphisms to a special subset of $\mathscr{C}$ associated with each subgroup of Γ.

Definition. Let N be a normal subgroup of Γ. The *quasi-level*, $ql(N)$, of N is the subset

$$ql(N) = \{c \in \mathscr{C} : T(c) \in N\}.$$

The quasi-level of an arbitrary subgroup S of Γ is defined to be $ql(N_S)$, where N_S is the *core* of S, i.e. the largest normal subgroup of Γ contained in S.

Then the level $l(S)$ is the largest $\mathscr{C}$-ideal contained in $ql(S)$. In some cases this containment is an equality. For example, it is clear that $l(\Gamma(\mathfrak{q})) = ql(\Gamma(\mathfrak{q})) = \mathfrak{q}$, for all $\mathscr{C}$-ideals $\mathfrak{q}$.

Obviously, inner automorphisms do not change the level of S since they respect N_S. If ψ is a ring automorphism of $\mathscr{C}$ and Ψ the corresponding standard automorphism of Γ, then $\Psi(S)$ has level $\psi(l(S))$. In particular, Ψ does not change the degree of the level. The main idea of this section and the next ones will be to use non-standard automorphisms of Γ that have a completely different effect on the level. So they cannot be contained in the group generated by the inner and standard ring automorphisms.

Conjugating by the diagonal matrices $L(\alpha, 0)$ we deduce the following.

Lemma 3.1. *Let S be a subgroup of Γ. Let $u, v \in ql(S)$ and $\alpha \in k^*$. Then*

(i) $u - v \in ql(S)$,
(ii) $\alpha^2 u \in ql(S)$.

As defined in [8], we say that $ql(S)$ is a *quasi-subspace* of $\mathscr{C}$. It is clear that every subspace of $\mathscr{C}$ is a quasi-subspace. Conversely, it is also clear that, when char $k \neq 2$ or k is perfect, every quasi-subspace is a subspace. However, it is not difficult [8, p. 287] to find examples of quasi-subspaces which are not subspaces.

Subgroups of level $\mathscr{C}$ have a number of special properties.

Lemma 3.2. *Suppose that k has at least four elements. Let S be a subgroup of Γ. The following are equivalent*:

(i) $ql(S) \cap k \neq \{0\}$,
(ii) $ql(S) = \mathscr{C}$,
(iii) $N_S \cap SL_2(k) \nleqslant \{\pm I_2\}$.

Proof. If (iii) is satisfied the simplicity of $PSL_2(k)$ implies that

$$SL_2(k) \leqslant \{\pm I_2\} N_S.$$

Let $c \in \mathscr{C}$. Choose $\alpha \in k^*$, where $\alpha \neq \pm 1$. Then

$$T(c) = L(\alpha, 0) T(c') L(\alpha^{-1}, 0) T(-c') \in N_S,$$

where $c' = c(\alpha^2 - 1)^{-1}$. Thus $\Delta(\mathscr{C}) \leqslant S$. The rest of the proof is obvious. □

The restriction here on k is necessary. By [8, Lemma 3.2(ii)] Lemma 3.2 does not hold for $\mathscr{C} = k[t]$, when k has two or three elements.

Lemma 3.3. *Let S be a subgroup of finite index in Γ.*

(i) *If k is infinite*, *then $ql(S) = \mathscr{C}$.*

(ii) *If* $k = \mathbb{F}_q$, *then* $ql(S)$ *is a* k-*subspace of* $\mathscr{C}$ *of finite codimension* r, *say. Moreover*,

$$q^r \leqslant |\Gamma : N_S|.$$

Proof. If $ql(S) \neq \mathscr{C}$ then, by Lemma 3.2,

$$N_S \cap SL_2(k) \leqslant \{\pm I_2\}.$$

Thus, (i) follows from

$$|SL_2(k) : N_S \cap SL_2(k)| \leqslant |\Gamma : N_S| < \infty.$$

For the second part we note that, since $U(ql(S)) = N_S \cap U(\mathscr{C})$, we have

$$q^r \leqslant |\mathscr{C} : ql(S)| = |U(\mathscr{C}) : U(ql(S))| = |U(\mathscr{C}) : N_S \cap U(\mathscr{C})| \leqslant |\Gamma : N_S|. \qquad \square$$

If, for any k, the fundamental group of the quotient graph $\Gamma\backslash X$ is non-trivial, the proof of [11, Theorem 1.2] shows that Γ has finite index subgroups of quasi-level $\mathscr{C}$ and any index.

We now show how non-standard automorphisms can be used to prove that “almost all” subspaces of $\mathscr{C}$ can be realized as the quasi-level of some subgroup of Γ. This involves the following straightforward lemma.

Lemma 3.4. *Let* V_0 *be any non-trivial finite-dimensional subspace of* $\mathscr{C}$. *Then there exist uncountably many subspaces* W *of* $\mathscr{C}$ *such that*

$$\mathscr{C} = V_0 \oplus W.$$

Equivalently, *there exist uncountably many* k-*automorphisms of* $\mathscr{C}$ *which fix* V_0.

We now choose one of the (infinitely many) non-zero $\mathscr{C}$-ideals, $\mathfrak{q}_0$, for which $\mathscr{C}(n_0) \cap \mathfrak{q}_0 = \{0\}$. Then there exists a finite-dimensional subspace $\mathscr{C}_0$ of $\mathscr{C}$, containing $\mathscr{C}(n_0)$, such that

$$\mathscr{C} = \mathscr{C}_0 \oplus \mathfrak{q}_0.$$

Theorem 3.5. *With the above notation*, *let* W *be one of the uncountably many subspaces of* $\mathscr{C}$ *such that*

$$\mathscr{C} = \mathscr{C}_0 \oplus W.$$

Then there exists a normal subgroup N *of* Γ *such that*

$$ql(N) = W.$$

Proof. Let $M = \Gamma(\mathfrak{q}_0)$ so that $ql(M) = \mathfrak{q}_0$. By Lemma 3.4 there exists a k-automorphism ϕ of $\mathscr{C}$, which fixes $\mathscr{C}_0$, such that $\phi(\mathfrak{q}_0) = W$. Let Φ be the automorphism of Γ induced by ϕ, as in Theorem 2.1. Then

$$ql(\Phi(M)) = \phi(\mathfrak{q}_0) = W. \qquad \square$$

The simplest cases of Theorem 3.5 arise when it is possible to choose $\mathscr{C}_0 = k$.

Corollary 3.6. *When k is finite, Γ has uncountably many finite index subgroups of level zero.*

Proof. In this case $\mathscr{C}$ has only countably many ideals. Consequently, there are uncountably many subspaces W as in the proof of Theorem 3.5 which do not contain any non-zero $\mathscr{C}$-ideal. □

Remark 3.7. Corollary 3.6 represents an anomaly in the following sense. Let A be an arithmetic Dedekind domain. (Apart from $A = \mathscr{C}$ the only other examples with finitely many units are $A = \mathbb{Z}$ and $A = \mathcal{O}_d$, the ring of integers in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$. Examples of such domains with infinitely many units include $A = \mathbb{Z}[p^{-1}]$, where p is a rational prime, and the Laurent polynomial ring, $k[t, t^{-1}]$, where $k = \mathbb{F}_q$.) The level of a subgroup of $SL_2(A)$ can be defined in an identical way. However, if $A \neq \mathscr{C}$, it is well-known that the level of a finite index subgroup of $SL_2(A)$ is always non-zero.

4. Level zero subgroups of small index

Throughout this section we assume that $k = \mathbb{F}_q$, with $p = \mathrm{char}(\mathbb{F}_q)$. Here we are concerned primarily with the minimal index of a non-congruence subgroup of level zero. It turns out that in nearly all cases this index is greater than $ncs(\mathscr{C})$. In [10–12] we determine $ncs(\mathscr{C})$. In most cases it turns out to be 2.

We note that any normal subgroup of Γ of index relatively prime to p must have level $\mathscr{C}$. (It contains all the matrices $T(c)$ since each has order p.) Thus, in many cases $ncs(\mathscr{C})$ can only be realized by a subgroup of level $\mathscr{C}$. For subgroups whose level is not $\mathscr{C}$ we have the following.

Lemma 4.1.

(a) *The minimal index of a subgroup S in Γ of level different from $\mathscr{C}$ is at least $m(SL_2(k))$.*
(b) *If $q > 3$, then the minimal index of a normal subgroup N in Γ of level different from $\mathscr{C}$ is at least $|PSL_2(k)|$.*

Proof. (a) There exists a subgroup H of Γ, conjugate to $E_2(\mathscr{C})$, such that $H \cap S$ is a proper subgroup of finite index in H. Thus,

$$|\Gamma : S| \geqslant |H : (H \cap S)| \geqslant m(SL_2(k[t])) = m(SL_2(k)).$$

Here the second inequality follows from the fact that $E_2(\mathscr{C}) \cong SL_2(k[t])$. (See [12, Lemma 2.1].) The final equality is proved in [10].

(b) Follows from Lemma 3.2. □

As we now show these lower bounds can be attained by subgroups of both zero and non-zero levels.

Lemma 4.2. *Suppose that $q \leqslant 3$. With the above notation, let V be any hyperplane of $\mathscr{C}$ containing $\mathscr{C}(n_0)$. Then there exists a normal subgroup of index q in Γ whose quasi-level is V.*

Proof. Let $Z = \{\pm I_2\}$. We note that, for every subspace W of $\mathscr{C}$,

$$U(W) \cong W^+.$$

It follows from Theorems 2.1 and 2.2 that

$$\Gamma = A \underset{C}{*} B,$$

where $B = Z \times U(\mathscr{C})$ and $C = Z \times U(\mathscr{C}(n_0))$. As in the proof of Theorem 2.4, the k-epimorphism from V onto k, whose kernel is V, extends in a natural way to an epimorphism from Γ onto k, whose kernel has the desired properties. □

We recall that $m(SL_2(k)) = q$ when $q \leqslant 3$.

Theorem 4.3. *Suppose that $q \leqslant 3$. Then*

(a) *Γ has uncountably many normal subgroups of level zero and index q.*
(b) *For every maximal ideal $\mathfrak{m}$ of $\mathscr{C}$ for which $\deg(\mathfrak{m}) > \dim_k(\mathscr{C}(n_0))$, there exists at least one normal non-congruence subgroup of Γ of level $\mathfrak{m}$ and index q.*

Proof. (a) Since $\mathscr{C}$ has only countably many ideals, there exist uncountably many hyperplanes in $\mathscr{C}$ each containing $\mathscr{C}(n_0)$ but not containing any non-zero ideal. The result follows from Lemma 4.2.

(b) The hypothesis ensures that there exists a hyperplane W in $\mathscr{C}$ which contains $\mathfrak{m}+\mathscr{C}(n_0)$. By Lemma 4.2 there exists a normal subgroup N of Γ of index q, quasi-level W and level $\mathfrak{m}$. If N is a congruence subgroup it contains $\Gamma(\mathfrak{m})$ by Theorem 1.1. Now $\Gamma/\Gamma(\mathfrak{m}) \cong SL_2(\mathbb{F}_{q'})$, where $q' \geqslant 4$, which has no normal subgroup of index q. It follows that N is a non-congruence subgroup. □

We now deal with the lower bound in Lemma 4.1(b).

Lemma 4.4. *Suppose that $\mathscr{C}$ has a maximal ideal $\mathfrak{m}$ with $\deg(\mathfrak{m}) = 1$. Let W be any hyperplane in $\mathscr{C}$ containing $\mathfrak{m} \cap \mathscr{C}(n_0)$ but not containing k. Then there exists a normal subgroup N of Γ of quasi-level W such that*

$$N \cong \Gamma(\mathfrak{m}).$$

Proof. It is clear that

$$\mathscr{C} = W \oplus k = \mathfrak{m} \oplus k,$$

from which it follows that

$$\mathscr{C}(n_0) = (W \cap \mathscr{C}(n_0)) \oplus k = (\mathfrak{m} \cap \mathscr{C}(n_0)) \oplus k.$$

We deduce that there exists a k-automorphism, ψ, of $\mathscr{C}$, fixing $\mathscr{C}(n_0)$, such that

$$\psi(\mathfrak{m}) = W.$$

The proof follows from Theorem 2.4. □

Proposition 4.5. *Suppose that $q > 3$ and that K has a place $\infty' \neq \infty$ of degree 1. Then:*

(a) *There exist uncountably many normal subgroups N of level zero with $\Gamma/N \cong PSL_2(k)$. There exist uncountably many level zero subgroups of index $m(SL_2(k))$ in Γ.*
(b) *For almost all maximal ideals $\mathfrak{m}$ of $\mathscr{C}$, there exists a normal non-congruence subgroup N of level $\mathfrak{m}$ with $\Gamma/N \cong PSL_2(k)$ and a non-congruence subgroup of level $\mathfrak{m}$ and index $m(SL_2(k))$ in Γ.*

Proof. Let $\mathfrak{m}'$ be the maximal $\mathscr{C}$-ideal determined by ∞'. Then $\Gamma/\Gamma(\mathfrak{m}') \cong SL_2(k)$.

(a) Clearly, $\mathscr{C}$ has uncountably many hyperplanes each containing $\mathfrak{m}' \cap \mathscr{C}(n_0)$ but not k or any non-zero $\mathscr{C}$-ideal. There exist uncountably many normal subgroups N of the required type by Lemma 4.4.
The simplicity of $PSL_2(k)$ ensures that any proper subgroup of Γ containing such an N is also non-congruence of level zero.
(b) We note that $\dim_k(\mathscr{C}(n_0)/\mathfrak{m}' \cap \mathscr{C}(n_0)) = 1$. If $\deg(\mathfrak{m})$ is big enough, we have

$$\mathfrak{m} \cap \mathscr{C}(n_0) = \{0\} \quad \text{and} \quad \deg(\mathfrak{m}) > \dim(\mathscr{C}(n_0)).$$

This ensures that there exists a hyperplane W of $\mathscr{C}$ containing $(\mathfrak{m}' \cap \mathscr{C}(n_0)) \oplus \mathfrak{m}$.

By Lemma 4.4 there exists a normal subgroup M of Γ isomorphic to $\Gamma(\mathfrak{m}')$ of quasi-level W and (hence) level $\mathfrak{m}$. Let $N = ZM$. Then N has level $\mathfrak{m}$ and $|\Gamma : N| = |PSL_2(k)|$.

If N is a congruence subgroup then N contains $\Gamma(\mathfrak{m})$, by Theorem 1.1. But $\Gamma/\Gamma(\mathfrak{m}) \cong PSL_2(\mathbb{F}_{q'})$, where $q' > q$, which has no normal subgroup of index $|PSL_2(k)|$. Hence N is a non-congruence subgroup which is contained in a subgroup S of index $m(SL_2(k))$. Clearly, S is also a non-congruence subgroup of level $\mathfrak{m}$. □

Remark 4.6. By the Hasse–Weil bound (see for example [15, Theorem V.2.3]) the condition in Proposition 4.5 is always satisfied if $g < \frac{1}{2}\sqrt{q}$. But there are also many rings $\mathscr{C}$ which have no ideals of degree 1. For $g = 1$, $q > 3$ the only example of such a ring is

$$\mathbb{F}_4[x, y] \quad \text{with } y^2 + y = x^3 + \alpha \quad \text{where } \alpha \text{ generates } \mathbb{F}_4^*.$$

In this specific case the conclusions of Proposition 4.5 hold nevertheless by the proof of the next lemma.

We wish to list all those $ncs(\mathscr{C})$ which are attained by subgroups of level zero. For this we require one further lemma.

Lemma 4.7. *Let $q = 4$ and $g = \delta = 1$. Then Γ has uncountably many normal subgroups N of level zero with $\Gamma/N \cong PSL_2(\mathbb{F}_4)$.*

Proof. This follows from the fact that there is a surjective group homomorphism from Γ to $E_2(\mathscr{C}) \cong SL_2(\mathbb{F}_4[t])$. (Compare with [12, Lemma 2.1 and Theorem 5.3]). □

Corollary 4.8.

(a) *There are uncountably many subgroups of level zero and index* $ncs(\mathscr{C})$ *for each of the following cases*:
  (i) $g = 0$, $\delta \leqslant 2$,
  (ii) $q = 2$,
  (iii) $\mathscr{C} \cong \mathbb{F}_4[x, y]$ *with* $y^2 + y = x^3 + \alpha$ *where* α *generates* $\mathbb{F}_4^*$,
  (iv) $\mathscr{C} \cong \mathbb{F}_4[x, y]$ *with* $y^2 + xy = x^3 + \alpha x + 1$ *where* α *generates* $\mathbb{F}_4^*$.
  In all other cases the minimal index of a subgroup of level zero is greater than $ncs(\mathscr{C})$.

(b) *The minimal index of a normal non-congruence subgroup is realized by a normal subgroup of level zero only in cases* (i) *and* (ii).

Proof. (a) We combine all the results of this section together with the explicit values of $ncs(\mathscr{C})$ given in [12].

Part (b) is proved in a similar way. □

5. Non-congruence subgroups of non-zero level

Throughout this section we again assume that $k = \mathbb{F}_q$. We are primarily concerned here with the minimal index of a non-congruence subgroup of a prescribed non-zero level, especially one of level $\mathscr{C}$.

In [11] we used the following lemma to prove (in a not very constructive way) the existence of certain non-congruence subgroups. As usual G^{ab} denotes the abelianization of a group G.

Lemma 5.1. *If the* (*free abelian*) *rank of* $\Gamma(\mathfrak{a})^{ab}$ *is positive*, *then*, *for every integer* $n > 1$, *there exists a non-congruence subgroup* S *of* Γ *of level* $\mathfrak{a}$ *with* $|\Gamma(\mathfrak{a}) : S| = n$.

In particular, *if* Γ^{ab} *itself has positive rank*, *then* Γ *has a* (*normal*) *non-congruence subgroup of index* 2 *and level* $\mathscr{C}$.

Proof. Consider the chain of canonical epimorphisms $\Gamma(\mathfrak{a}) \to \Gamma(\mathfrak{a})^{ab} \to \mathbb{Z}^r$, where r is the rank of $\Gamma(\mathfrak{a})^{ab}$. In $\mathbb{Z}^r$ we can choose a (normal) subgroup of index n. Its preimage in $\Gamma(\mathfrak{a})$ contains $\Delta(\mathfrak{a})$, since $\Delta(\mathfrak{a})$ is generated by torsion elements, and it is a non-congruence subgroup by Theorem 1.1 unless $n = 1$. □

Before applying this lemma, we first look at some special cases where Γ^{ab} has zero rank. (See [11].)

Lemma 5.2. *Let* $q = 2$.

(a) *If* $g = 0$ *and* $\delta = 3$, *then there exist uncountably many non-congruence subgroups of level* $\mathscr{C}$ *and index* 2.

(b) *If* $g = \delta = 1$, *then* $\mathscr{C}$ *is the affine coordinate ring of an elliptic curve* E *over* $\mathbb{F}_2$. *If* $\mathscr{C}$ *has a* (*maximal*) *ideal of degree* 1, *i.e. if* $\#E(\mathbb{F}_2) > 1$, *then* Γ *has uncountably many non-congruence subgroups of level* $\mathscr{C}$ *and index* 2.

(c) *The* (*up to isomorphism*) *only case in* (b) *where* $\mathscr{C}$ *has no ideals of degree* 1 *is*

$$\mathscr{C} = \mathbb{F}_2[x, y] \quad \textit{with } y^2 + y = x^3 + x + 1.$$

For every maximal ideal $\mathfrak{m}$ *of this* $\mathscr{C}$, *there exists a non-congruence subgroup of level* $\mathfrak{m}$ *and index* 2, *but the smallest index of a* (*normal*) *subgroup of level* $\mathscr{C}$ *is* 3.

Proof. (a) By [12, Theorem 4.5] in this case we have

$$\Gamma = E_2(\mathscr{C}) * \Gamma^* * \Gamma^{**},$$

where Γ^* and Γ^{**} are $\mathbb{F}_2$-vector spaces of countably infinite dimension. If N is the normal subgroup generated by $E_2(\mathscr{C})$ and Γ^*, then $\Gamma/N \cong \Gamma^{**}$, and Γ^{**} has uncountably many subgroups of index 2.

(b) We adopt the notation used in [12, Section 5]. Note that the groups $\Delta(\alpha)$ in that paper are different from the groups $\Delta(\mathfrak{a})$ in the present paper. By [12, Theorem 5.2] we have

$$\Gamma = (B_2(\mathscr{C}) \underset{B_2(k)}{*} SL_2(k)) * \Delta(0) * \Delta(1).$$

If $\#E(\mathbb{F}_2) > 1$, we see (from the description in [12, Theorem 5.3]) that at least one of the groups $\Delta(0)$, $\Delta(1)$ has uncountably many subgroups of index 2.

(c) The fact that this is the only elliptic curve over $\mathbb{F}_2$ with only one rational point is well known. (See [14, p. 117, Exercise 3].)

For the other statements we use the amalgamated product from part (b). We extend $B_2(\mathfrak{m})$ to a complement U of $B_2(\mathbb{F}_2)$ in $B_2(\mathscr{C})$. Then the normal subgroup S of Γ generated by $\Delta(0)$, $\Delta(1)$, U and the elements of order 3 in $SL_2(\mathbb{F}_2)$ has level $\mathfrak{m}$ and index 2. Now $|\mathscr{C}/\mathfrak{m}| \geqslant 4$ and so $\Gamma/\Gamma(\mathfrak{m}) \cong SL_2(\mathscr{C}/\mathfrak{m})$ has no subgroups of index 2. So S cannot contain $\Gamma(\mathfrak{m})$, and S is therefore a non-congruence subgroup by Theorem 1.1.

The last statement follows from the fact that in this case $\Delta(0)$ and $\Delta(1)$ are groups of order 3. (See [12, Theorem 5.2].) □

Theorem 5.3. *If* $g > 0$ *or* $\delta > 2$, *then*, *with the exception of the* "*elliptic*" *case discussed in Lemma* 5.2(c), *the group* Γ *always has a normal non-congruence subgroup of level* $\mathscr{C}$ *and index* $ncs(\mathscr{C})$.

Proof. First, we treat the cases where q is even and (g, δ) is $(0, 3)$ or $(1, 1)$. If $4|q$, we have shown in [12] that Γ contains a normal non-congruence subgroup of level $\mathscr{C}$ and index $ncs(\mathscr{C})$. For $q = 2$ see Lemma 5.2.

In all other cases Γ has positive rank and so Lemma 5.1 applies. □

Corollary 5.4.

(a) *The minimal index of a normal non-congruence subgroup in* Γ *can always be attained by a normal non-congruence subgroup of non-zero level.*
(b) *The minimal index* $ncs(\mathscr{C})$ *can always be attained by a non-congruence subgroup of non-zero level.*

Proof. Follows from Theorems 4.3, 5.3 and Proposition 4.5. □

Clearly, for any Γ every non-zero $\mathscr{C}$-ideal is the level of a congruence subgroup, which gives rise to the following question. Is this also true for the non-congruence subgroups of Γ?

Theorem 5.5.

(a) $SL_2(k[t])$ *has no non-congruence subgroups of level* $\mathfrak{a}$ *if and only if* $\deg(\mathfrak{a}) \leqslant 1$. *If* $\deg(\mathfrak{a}) > 1$, *the number of non-congruence subgroups of level* $\mathfrak{a}$ *is countably infinite*.
(b) *Let* $g = 0$ *and* $\delta = 2$. *If* $q \leqslant 3$, *then there exist uncountably many normal non-congruence subgroups of level* $\mathscr{C}$ *and index* q *in* Γ. *But if* $q > 3$, *then* Γ *has no non-congruence subgroups of level* $\mathscr{C}$. *For any* q *there are infinitely many non-congruence subgroups of level* $\mathfrak{a}$, *for all* $\mathscr{C}$-*ideals* $\mathfrak{a}$.
(c) *If* $g > 0$ *or* $\delta > 2$, *then* Γ *has non-congruence subgroups of every non-zero level* $\mathfrak{a}$.

Proof. (a) Since $\Gamma = SL_2(k[t])$ is generated by elementary matrices, it follows that $\Delta(\mathscr{C}) = \Gamma$.

Suppose that $\deg(\mathfrak{m}) = 1$. Then Γ is generated by $\Delta(\mathfrak{m})$ and $SL_2(k)$ (again since Γ is generated by elementary matrices). So we see that

$$\Gamma/\Delta(\mathfrak{m}) \cong \Gamma/\Gamma(\mathfrak{m}) \cong SL_2(k).$$

Thus $\Gamma(\mathfrak{m}) = \Delta(\mathfrak{m})$.

If however $\deg(\mathfrak{a}) > 1$, then $\Gamma(\mathfrak{a})^{ab}$ has positive rank by [5, Corollary 5.8]. By Lemma 5.1 then infinitely many non-congruence subgroups of $SL_2(k[t])$ of level $\mathfrak{a}$.

On the other hand, $SL_2(k[t])/\Delta(\mathfrak{a})$ is generated by elementary matrices whose off-diagonal entries can be chosen from a system of representatives of $k[t]$, modulo $\mathfrak{a}$. Hence $SL_2(k[t])/\Delta(\mathfrak{a})$ is finitely generated. Since a finitely generated group has at most countably many subgroups of finite index this implies that there are only countably many subgroups of level $\mathfrak{a}$ and finite index in $SL_2(k[t])$.

(b) We refer to the (complicated) amalgamated product given in [12, Theorem 3.3]. If $q \leqslant 3$, then in this product the group Γ^* is the direct sum of L and a k-vector space V of countably infinite dimension. If N is the normal subgroup of Γ generated by Γ_∞, Γ_0 and Γ_1^*, then $\Delta(\mathscr{C}) \subseteq N$ and $\Gamma/N \cong V$. Now V has uncountably many subgroups of index q.

For $q > 3$ it was shown in [12, Lemma 3.5] that the normal subgroup of Γ generated by $SL_2(k)$ is Γ. This immediately implies $\Delta(\mathscr{C}) = \Gamma$ and hence that Γ has no non-congruence subgroups of level $\mathscr{C}$.

From [4, Theorem 5.11, p. 90] we see that for every non-trivial ideal $\mathfrak{a}$ of $\mathscr{C}$ the rank of $\Gamma(\mathfrak{a})^{ab}$ is positive. Hence by Lemma 5.1 there are infinitely many non-congruence subgroups of level $\mathfrak{a}$.

(c) We have already seen in Theorem 5.3 that in this case there is always a non-congruence subgroup S of level $\mathscr{C}$. Then $S \cap \Gamma(\mathfrak{a})$ is a non-congruence subgroup of level $\mathfrak{a}$. □

Corollary 5.6. *If* Γ *has a non-congruence subgroup of level* $\mathscr{C}$, *then it also has a non-congruence subgroup of level* $\mathscr{C}$ *and index* $ncs(\mathscr{C})$, *except for the* "*elliptic*" *case discussed in Lemma* 5.2(c).

Proof. Follows from Theorems 5.3 and 5.5. □

6. Principal ideal domains

We continue with the assumption that k is finite. As we shall see the ideal class group, $Cl(\mathcal{C})$, of (the Dedekind domain) $\mathcal{C}$ plays a central role in Serre's decomposition theorem [14, Theorem 10, p. 119]. The principal aim of this section is to establish a *group-theoretic* property particular to those Γ for which $Cl(\mathcal{C})$ is trivial.

Remark 6.1. By virtue of the exact sequence on [14, p. 104] it follows that $Cl(\mathcal{C})$ is trivial if and only if $\delta = 1$ and the *divisor class group* of K, $Jac(K)$, is trivial. (See [15, p. 16].)

From [7, Theorem 2] we see that apart from $\mathcal{C} \cong k[t]$ there are (up to isomorphism) only 4 other $\mathcal{C}$ with trivial ideal class group, namely

$\mathbb{F}_2[x, y]$ with $y^2 + y = x^3 + x + 1$,
$\mathbb{F}_2[x, y]$ with $y^2 + y = x^5 + x^3 + 1$,
$\mathbb{F}_3[x, y]$ with $y^2 = x^3 - x - 1$,
$\mathbb{F}_4[x, y]$ with $y^2 + y = x^3 + \alpha$ where α generates $\mathbb{F}_4^*$.

(There are a few more fields K with trivial divisor class group, but they do not have any places of degree 1.)

The proofs in this section do not use the explicit description in Remark 6.1.

We require a matrix version [9] of [14, Theorem 10, p. 119]. We begin with some definitions from [9]. From now on we put

$$G = GL_2(\mathcal{C}).$$

Definition. For each $s \in K^*$, we put

$$S(s) := \left\{ \begin{bmatrix} \alpha + sc & (\beta - \alpha)s - s^2 c \\ c & \beta - sc \end{bmatrix} : \alpha, \beta \in k^*, \right. \\ \left. c \in \mathcal{C} \cap \mathcal{C}s^{-1} \cap \left((\beta - \alpha)s^{-1} + \mathcal{C}s^{-2} \right) \right\}.$$

Then $S(s)$ is a subgroup of G with a normal subgroup

$$U(s) := \left\{ \begin{bmatrix} 1 + sc & -s^2 c \\ c & 1 - sc \end{bmatrix} : c \in \mathcal{C} \cap \mathcal{C}s^{-1} \cap \mathcal{C}s^{-2} \right\}.$$

We put

$$S(\infty) := \left\{ \begin{bmatrix} \alpha & c \\ 0 & \beta \end{bmatrix} : \alpha, \beta \in k^*, c \in \mathcal{C} \right\}.$$

Then $S(\infty)$ is a subgroup of G with a normal subgroup

$$U(\infty) := \{T(c) : c \in \mathcal{C}\}.$$

Our results depend on a decomposition for G of the following type.

Definition. We say that a group H is the *star-product* of its subgroups $H_0, H_1, \cdots, H_n$, where $n \geqslant 1$, written

$$H = Star(H_0; H_1, \ldots, H_n),$$

if

$$H \cong \pi(G(-), T),$$

the *fundamental group*, [2, p. 12], of the (star-shaped) *tree of groups*, $(G(-), T)$, where

(i) $V(T) = \{v_0, v_1, \ldots, v_n\}$,
(ii) $E(T) = \{e_1, \ldots, e_n\}$, with e_i joining v_0 and v_i $(1 \leqslant i \leqslant n)$,
(iii) $G(v_j) = H_j$ $(0 \leqslant j \leqslant n)$,
(iv) $G(e_i) = H_0 \cap H_i$ $(1 \leqslant i \leqslant n)$.

(Less precisely H is "the free product of $H_0, H_1, \ldots, H_n$, with H_0 and H_i amalgamated along their common subgroup $H_0 \cap H_i$, where $1 \leqslant i \leqslant n$.")

We put

$$\widehat{K} = \mathbb{P}_1(K) = K \cup \{\infty\}.$$

(Note that here the symbol "∞" is used in a different context than earlier.) The group G acts on $\widehat{K}$ (as linear fractional transformations) and it is well-known that this provides a one–one correspondence

$$G \backslash \widehat{K} \leftrightarrow Cl(\mathscr{C}).$$

Since k is finite it is also well-known that $Cl(\mathscr{C})$ is finite.

The group G also acts [14, Chapter II, Section 1] on its associated *Bruhat–Tits tree*, X, and the structure of the quotient graph $G \backslash X$ leads, via the theory of groups acting on trees, to the decomposition theorem [14, Theorem 10, p. 119]. It is known that, when k is finite, the stabilizer in G of every vertex (and hence every edge) of X is *finite*. (See [14, Proposition 2, p. 76].)

Theorem 6.2. *With the above notation, there exists a finite subset $\mathscr{S}$ of $\widehat{K} - k$, containing ∞, in one–one correspondence with $Cl(\mathscr{C})$, together with elements $g_\sigma \in G$, where $\sigma \in \mathscr{S}$ and $g_\infty = I_2$, and a subgroup S_0 of G such that*

$$G = Star(S_0;\ \ g_\sigma S(\sigma) g_\sigma^{-1}, (\sigma \in \mathscr{S})),$$

where

$$S_0 \cong \pi(G(-), Y),$$

the fundamental group of a graph of groups $(G(-), Y)$, with Y a finite (connected) subgraph of $G \backslash X$.

Moreover, $S_0 \cap g_\sigma S(\sigma) g_\sigma^{-1}$ is finite, for all $\sigma \in \mathscr{C}$.

Proof. We denote $G\backslash X$ by $\bar{X}$. The structure of $\bar{X}$ is given by [14, Theorem 9, p. 106]. (See also [9, Theorem 4.7].) Using a *lift*, $j : \bar{T} \to X$, of a maximal tree $\bar{T}$ of $\bar{X}$, the decomposition for G [14, Theorem 10, p. 119] follows from [14, Theorem 13, p. 55]. (For a matrix version see [9, Theorem 5.1].) Conjugating (if necessary) we may choose $g_\infty = I_2$.

The assertion that S_0 is the fundamental group of a finite graph of groups follows from the fact that

$$\{e \in E(\bar{X}) : e \notin E(\bar{T})\}$$

is *finite*. (See [14, Corollary 4, p. 108] or [9, Lemma 5.2].) For the remainder see [9, Theorem 5.1, Lemma 1.2]. □

We will now obtain a "restricted" version of Theorem 6.2 for the (normal) subgroup $\Gamma(\mathfrak{q})$ of G. For this we require a number of lemmas. We write *almost all* for *all but finitely many*.

Lemma 6.3. *Let S be a finite subgroup of G. Then, for almost all* $\mathfrak{q}$,

$$\Gamma(\mathfrak{q}) \cap S = \{I_2\}.$$

Proof. We note that $X = (x_{ij})$ lies in $\Gamma(\mathfrak{q})$ if and only if

$$x_{11} - 1, \quad x_{22} - 1, \quad x_{12}, \quad x_{21} \in \mathfrak{q}. \qquad \square$$

Lemma 6.4. *For almost all* $\mathfrak{q}$, *the group*

$$\Gamma(\mathfrak{q}) \cap S_0$$

is finitely generated free (*possibly trivial*).

Proof. We recall from Theorem 6.2 that

$$S_0 = \pi(G(-), Y),$$

where Y is a finite subgraph of $\bar{X}$. Let Y' be the lift in X of a maximal tree of Y. By Lemma 6.3 it follows that, for almost all $\mathfrak{q}$, the stabilizer in $\Gamma(\mathfrak{q})$ of each of the vertices of Y' is trivial. We now fix such a $\mathfrak{q}$.

The above presentation for S_0 determines a *tree*, T_0, (its "universal covering") on which S_0 acts, such that

$$S_0\backslash T_0 \cong Y.$$

(See [14, p. 51].) Then $S_0 \cap \Gamma(\mathfrak{q})$ acts on T_0 such that all its vertex stabilizers are trivial. It follows that $S_0 \cap \Gamma(\mathfrak{q})$ is free. In addition, S_0 and hence $S_0 \cap \Gamma(\mathfrak{q})$ are finitely generated. □

Lemma 6.5. *Let* $\mathfrak{q}$ *be any proper* $\mathscr{C}$*-ideal. Then*

$$\begin{bmatrix} \alpha + sc & (\beta - \alpha)s - s^2c \\ c & \beta - sc \end{bmatrix} \in \Gamma(\mathfrak{q})$$

if and only if $\alpha = \beta = 1$ *and* $c \in \mathfrak{q} \cap \mathfrak{q}s^{-1} \cap \mathfrak{q}s^{-2}$.

Proof. If the above matrix belongs to $\Gamma(\mathfrak{q})$, then

$$\alpha\beta = 1 \text{ and } \alpha + \beta \equiv 2 \pmod{\mathfrak{q}}.$$

Since $\mathfrak{q} \neq \mathscr{C}$ it follows that $\alpha + \beta = 2$ and hence that $\alpha = \beta = 1$. $\square$

Definition. For each $\mathfrak{q}$ and each $s \in K^*$, we put $\mathfrak{q}_s := \mathfrak{q} \cap \mathfrak{q}s^{-1} \cap \mathfrak{q}s^{-2}$ and

$$U(\mathfrak{q}_s) := \left\{ \begin{bmatrix} 1+cs & -cs^2 \\ c & 1-cs \end{bmatrix} : c \in \mathfrak{q}_s \right\}.$$

We put $\mathfrak{q}_\infty := \mathfrak{q}$ and

$$U(\mathfrak{q}_\infty) := \{T(c) : c \in \mathfrak{q}\}.$$

It is clear that, for all $\sigma \in \widehat{K}$,

$$U(\mathfrak{q}_\sigma) \cong (\mathfrak{q}_\sigma)^+.$$

With the notation of Theorem 4.1 we put

$$\bar{S}(\sigma) = g_\sigma S(\sigma) g_\sigma^{-1}$$

and

$$\bar{U}(\mathfrak{q}_\sigma) = \Gamma(\mathfrak{q}) \cap \bar{S}(\sigma) = g_\sigma U(\mathfrak{q}_\sigma) g_\sigma^{-1},$$

where $\sigma \in \mathscr{S}$.

Theorem 6.6. *For almost all non-zero* $\mathfrak{q}$, *there exists a system,* R_σ, *of right coset representatives for* G, $\mathrm{mod}(\Gamma(\mathfrak{q}) \cdot \bar{S}(\sigma))$, *and a finitely generated free subgroup* F *of* G *such that*

$$\Gamma(\mathfrak{q}) = F * \left(\mathop{*}_{\sigma \in \mathscr{S}} W(\mathfrak{q}_\sigma) \right),$$

where, for each $\sigma \in \mathscr{S}$,

$$W(\mathfrak{q}_\sigma) = \mathop{*}_{g \in R_\sigma} g \bar{U}(\mathfrak{q}_\sigma) g^{-1}.$$

Proof. We now fix one of the almost all, proper, non-zero $\mathfrak{q}$ for which Lemmas 6.3, 6.4 and 6.5 hold. We can now apply [3, Corollary 5.1] to the normal subgroup $\Gamma(\mathfrak{q})$ of the tree-product G. Then by Theorem 6.2

$$\Gamma(\mathfrak{q}) = F_0 * \left(\mathop{*}_{\sigma \in \mathscr{S}} W(\mathfrak{q}_\sigma) \right),$$

where

$$F_0 = \mathop{*}_{g \in R_0} g(\Gamma(\mathfrak{q}) \cap S_0) g^{-1},$$

for some system R_0 of right coset representatives for G, $\mathrm{mod}(\Gamma(\mathfrak{q}) \cdot S_0)$. The result follows from Lemma 6.4. $\square$

We now come to the main results in this section.

Theorem 6.7. *The group $\Gamma/\Delta(\mathfrak{q})$ is finitely generated, for all non-zero $\mathfrak{q}$, if and only if $\mathscr{C}$ is a principal ideal domain.*

Proof. Let $\mathfrak{q}$ be any ideal to which Theorem 6.6 applies and let $\bar{\Delta}(\mathfrak{q})$ be the normal subgroup of $\Gamma(\mathfrak{q})$ generated by

$$W(\mathfrak{q}_\infty) = \mathop{*}_{g \in R_\infty} gU(\mathfrak{q}_\infty)g^{-1}.$$

Then $\bar{\Delta}(\mathfrak{q})$ is the normal subgroup of G generated by $U(\mathfrak{q}_\infty)$. It is clear that $\Delta(\mathfrak{q}) \leqslant \bar{\Delta}(\mathfrak{q})$. Now consider any element

$$gT(c)g^{-1},$$

where $g \in G$ and $c \in \mathfrak{q}$. Then

$$g = dg',$$

where $g' \in \Gamma$ and $d = \mathrm{diag}(\alpha, 1)$ with $\alpha = \det\ g$. It is easily verified that

$$gT(c)g^{-1} = g_0 T(c')g_0^{-1},$$

where $g_0 = dg'd^{-1}$ and $c' = \alpha c$. We deduce that $\Delta(\mathfrak{q}) = \bar{\Delta}(\mathfrak{q})$ and hence that

$$\Gamma(\mathfrak{q})/\Delta(\mathfrak{q}) \cong F * \left(\mathop{*}_{\sigma \neq \infty} W(\mathfrak{q}_\sigma) \right).$$

Suppose that $\mathscr{S} = \{\infty\}$. Then

$$\Gamma(\mathfrak{q})/\Delta(\mathfrak{q}) \cong F$$

is finitely generated by Theorem 6.6. Hence $\Gamma/\Delta(\mathfrak{q})$ is finitely generated for all $\mathfrak{q}$, since $\Delta(\mathfrak{q}_1) \leqslant \Delta(\mathfrak{q}_2)$ whenever $\mathfrak{q}_1 \leqslant \mathfrak{q}_2$.

Suppose now that $\mathscr{S} \neq \{\infty\}$. Let $\sigma \in \mathscr{S} - \{\infty\}$. Then by Theorem 6.6 $\Gamma(\mathfrak{q})/\Delta(\mathfrak{q})$ maps onto

$$U(\mathfrak{q}_\sigma) \cong (\mathfrak{q}_\sigma)^+,$$

for almost all $\mathfrak{q}$. Now $(\mathfrak{q}_\sigma)^+$ is the additive group of a k-vector space of countably infinite dimension and consequently is not finitely generated. □

It is well-known [14, Lemma 11, p. 125] that Γ has uncountably many subgroups of finite index. How many of these have non-zero level depends on the ideal class number of $\mathscr{C}$.

Theorem 6.8. *The group Γ has at most countably many finite index subgroups of non-zero level if and only if $\mathscr{C}$ is a principal ideal domain.*

Proof. The subgroups of non-zero level $\mathfrak{q}$ are in bijection with the subgroups of $\Gamma/\Delta(\mathfrak{q})$. In addition, $\mathscr{C}$ has only countably many ideals $\mathfrak{q}$ (since they are at most 2-generated).

If $Cl(\mathscr{C})$ is trivial, then the result follows from Theorem 6.7. Suppose now that $Cl(\mathscr{C})$ is not trivial. Then, from the proof of Theorem 6.7, there exists a non-zero $\mathfrak{q}$ such that $\Gamma(\mathfrak{q})/\Delta(\mathfrak{q})$ maps onto the additive group of a k-vector space of countably infinite dimension. Such a space has uncountably many hyperplanes and so $\Gamma/\Delta(\mathfrak{q})$ has uncountably many subgroups of finite index. $\square$

References

[1] P.M. Cohn, On the structure of the GL_2 of a ring, Publ. Math. I.H.E.S. 30 (1966) 5–53.

[2] W. Dicks, M.J. Dunwoody, Groups Acting on Graphs, Cambridge University Press, Cambridge, 1989.

[3] J. Fischer, The subgroups of a tree product of groups, Trans. Amer. Math. Soc. 210 (1975) 27–50.

[4] E.-U. Gekeler, Drinfeld Modular Curves, Lecture Notes in Mathematics, vol. 1231, Springer, Berlin, Heidelberg, New York, 1986.

[5] E.-U. Gekeler, U. Nonnengardt, Fundamental domains of some arithmetic groups over function fields, Internat. J. Math. 6 (1995) 689–708.

[6] F. Grunewald, J. Schwermer, On the concept of level for subgroup of SL, over arithmetic rings, Israel J. Math. 114 (1999) 205–220.

[7] J. Leitzel, M. Madan, C. Queen, Algebraic function fields with small class number, J. Number Theory 7 (1975) 11–27.

[8] A.W. Mason, Normal subgroups of $SL_2(k[t])$ with or without free quotients, J. Algebra 150 (1992) 281–295.

[9] A.W. Mason, Serre's generalization of Nagao's theorem: an elementary approach, Trans. Amer. Math. Soc. 353 (2003) 749–767.

[10] A.W. Mason, On non-congruence subgroups of the analogue of the modular group in characteristic p, Ramanujan J. Math. 7 (2003) 141–144.

[11] A.W. Mason, A. Schweizer, The minimum index of a non-congruence subgroup of SL_2 over an arithmetic domain, Israel J. Math. 133 (2003) 29–44.

[12] A.W. Mason, A. Schweizer, The minimum index of a non-congruence subgroup of SL_2 over an arithmetic domain. II: The rank zero cases, J. London Math. Soc. 71 (2005) 53–68.

[13] I. Reiner, A new type of automorphism of the general linear group over a ring, Ann. Math. 66 (1957) 461–466.

[14] J.-P. Serre, Trees, Springer, Berlin, Heidelberg, New York, 1980.

[15] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.

[16] S. Takahashi, The fundamental domain of the tree of $GL(2)$ over the function field of an elliptic curve, Duke Math. J. 72 (1993) 85–97.